(12) UK Patent Application (19) GB (11) 2 372 921 (13) A

(43) Date of Printing by UK Office 04.09.2002

(21) Application No 0212745.4

(22) Date of Filing 07.11.2000

(30) Priority Data
(31) 09451504 (32) 30.11.1999 (33) US

(86) International Application Data
PCT/US2000/041995 En 07.11.2000

(87) International Publication Data
WO2001/041353 En 07.06.2001

(71) Applicant(s)
Sun Microsystems, Inc.
(Incorporated in USA - Delaware)
901 San Antonio Road, Palo Alto, California 94303,
United States of America

(72) Inventor(s)
Radia Perlman
Stephen Hanna

(74) continued overleaf

(51) INT CL^7
H04L 9/08 29/06

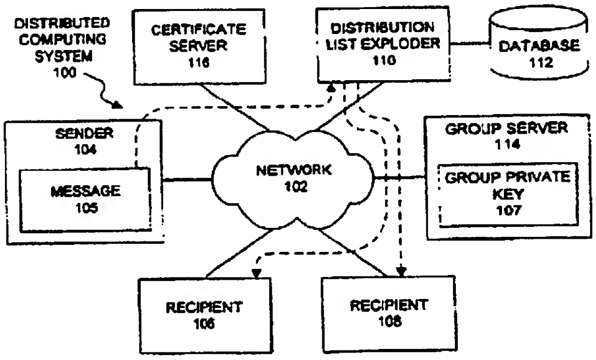
(52) UK CL (Edition T)
H4P PDCSC PPEB

(56) Documents Cited by ISA
HERFERT M:"SECURITY-ENHANCED MAILING LISTS" IEEE NETWORK, IEEE INC. NEW YORK,USvol.11,no3, 1 May 1997 (1997-05-01), pages 30-33, XP000689787 ISSN: 0890-8044 abstract page 30, right-hand column, line 8 - line 10 page 31, left-hand column,line 13 -righthand column, line 20
SERENELLI B ET AL:"SECURING ELECTRONIC MAIL SYSTEMS" SAN DIEGO, OCT.11-14, 1992 NEWYORK, IEEE,US, vol. CONF. 11, 11 October 1992 (1992-10-11), pages 677-680, XP000346673 ISBN: 0-7803-0586-8 table I

(56) and (58) continued overleaf

(54) Abstract Title
Method and apparatus for sending encrypted electronic mail through a distribution list exploder

(57) One embodiment of the present invention provides a system for sending an encrypted message through a distribution list exploder in order to forward the encrypted message to recipients on a distribution list. The system operates by encrypting the message at a sender using a message key to form an encrypted message. The system also encrypts the message key with a group public key to form an encrypted message key. The group public key is associated with a group private key to form a public key-private key pair associated with a group of valid recipients for the message. Next, the system sends the encrypted message and the encrypted message key to the distribution list exploder, and the distribution list exploder forwards the encrypted message to a plurality of recipients specified in the distribution list. After receiving the encrypted message and the encrypted message key, the recipient decrypts the encrypted message key to restore the message key. Next, the recipient decrypts the encrypted message using the message key to restore the message. In a variation on the above embodiment, the recipient decrypts the encrypted message key by sending the encrypted message key from the recipient to a group server, which holds the group private key. The group server decrypts the encrypted message key using the group private key to restore the message key, and returns the message key to the recipient in a secure manner.


DISTRIBUTED COMPUTING SYSTEM 100
CERTIFICATE SERVER 116
DISTRIBUTION LIST EXPLODER 110
DATABASE 112
SENDER 104
MESSAGE 105
NETWORK 102
GROUP SERVER 114
GROUP PRIVATE KEY 107
RECIPIENT 106
RECIPIENT 108